Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Олешко Єгора Сергійовича*

академічної групи *УБіт-15-1*

напряму підготовки *6.170103 Управління інформаційною безпекою*

спеціалізації

за освітньо-професійною програмою

на тему *Розробка політки безпеки інформації інформаційно - телекомунікаційної системи ТОВ «Охоронна фірма СТІНА»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. В.І. Корнієнко			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2019

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Олешку Єгору Сергійовичу*** **академічної групи** ***УБіт-15-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки *6.170103 Управління інформаційною безпекою*
(код і назва спеціальності)

на тему ***Розробка політки безпеки інформації інформаційно - телекомунікаційної системи ТОВ «Охоронна фірма СТІНА»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Провести обслідування об'єкту інформаційної діяльності ТОВ «Охоронна фірма СТІНА». Виявити загрози для інформаційної системи підприємства	20.03.2019
Розділ 2	Розробити політику безпеки для підприємства ТОВ «Охоронна фірма СТІНА»	30.05.2019
Розділ 3	Розрахувати капітальні витрати на програмне та апаратне забезпечення інформаційної системи підприємства	15.06.2019

Завдання видано _____ ст. викл. Мєшков В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 17.06.2019р.

Прийнято до виконання _____ Олешко Є.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., __ табл., __ додатків, __ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система (ІТС) ТОВ «Охоронна фірма СТІНА».

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності (ОІД).

Мета роботи (проекту): розробити політику безпеки інформації (ПБ) в ІТС ТОВ «Охоронна фірма СТІНА».

У першому розділі проведено аналіз нормативно-правової бази у сфері захисту інформації та визначена актуальність проблеми захисту інформації в ІТС комерційних підприємств, встановлені задачі на розробку комплексної системи захисту інформації КСЗІ, на ОІД, де циркулює інформація.

У спеціальній частині складено акт обстеження на об’єкті інформаційної діяльності, розглянуто загальні відомості про підприємство, його організаційну структуру, аналіз середовища функціонування об’єкта інформаційної діяльності, класифікована інформація, що обробляється у інформаційно-телекомунікаційній системі та наведено характеристику компонентів системи. Також розроблено моделі загроз та порушника безпеки інформації, проаналізовані ризики для інформації і сформовані основні положення політики безпеки інформації для комплексної системи захисту інформації.

В третьому розділі визначено економічну доцільність впровадження ПБ. Проведено розрахунки капітальних витрат, поточних витрат, оцінки величини збитку та загальний ефект від впровадження КСЗІ.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ.

РЕФЕРАТ

Пояснительная записка: __ с., __ рис., __ табл., __ прилож., __источников.

Объект разработки: информационно-телекоммуникационная система ООО «Охранная фирма СТЕНА».

Предмет: политика безопасности информации объекта информационной деятельности (ОИД).

Цель работы (проекта): разработать политику безопасности информации в ИТС ООО «Охранная фирма СТЕНА».

В первом разделе проведен анализ нормативно-правовой базы в сфере защиты информации и указана актуальность вопроса, поставлены задачи на внедрение системы защиты информации на объектах информационной деятельности, где циркулирует информация.

В специальной части составлен акт обследования на объекте информационной деятельности, рассмотрены общие сведения о предприятии, его организационная структура, анализ среды функционирования объекта информационной деятельности, классифицирована информация, обрабатываемая в информационно-телекоммуникационной системе, и приведено описание компонентов системы. Также разработаны модели угроз и нарушителя безопасности информации, проанализированы риски для информации и сформированы основные положения политики безопасности информации для комплексной системы защиты информации.

В третьем разделе определена экономическая целесообразность внедрения информационной политики безопасности. Проведены расчеты капитальных (фиксированных) расходов, текущих (эксплуатационных) расходов, оценки величины ущерба и общий эффект от внедрения системы информационной безопасности. Определены и проанализированы показатели экономической эффективности систему информационной защиты.

Практическое значение работы состоит в возможности ее использования для разработки КСЗИ на реальном ОИД. Результаты, полученные в дипломном проекте, могут быть использованы для разработки и внедрения КСЗИ на предприятии.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНОФРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, АКТ ОБСЛЕДОВАНИЯ.

ABSTRACT

An Explanatory Note: ____p., ___fig., ____tables., ____app., ___sources.

The object of this study is information and telecommunication system of the «Security company STINA» LLC.

The subject of this study: information security policy of information activity object.

The purpose of the study: developing the security policy in information and telecommunication system of the «Security company STINA» LLC.

The first part of the study contains an analysis of regulatory documentation in information security, set tasks for the implementation of the information security system for information activity object where the information circulates.

The main part of the study considers the general statements about the enterprise; organizational structure of the computer system is contained. Information activity object`s environment for the functioning; risk assessment; threat analysis of information security; main elements of the information security policy of information and telecommunication system are analyzed; the main regulations of the security policy are formulated.

In the economic part defines economic feasibility of implementing an information security policy. The calculations of capital (fixed) costs, current (operational) costs, a calculation of loss and the effect of the implementation of information security. Economic efficiency indicators of information system security are analyzed.

The analyses provide the opportunity to use the developed security policy for implementation in the information and telecommunication system of the enterprise.

INTEGRATED INFORMATION PROTECTION SYSTEM, INFORMATION SECURITY POLICY, INFORMATION OBJECTIVE, RISK ANALYSIS, THREAT MODEL, DISTURB MODEL, SURVEY ACT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ – комплексна система захисту інформації;

ПК – персональний комп’ютер;

ІзОД – інформація з обмеженим доступом;

ОС – обчислювальна система;

КЗЗ – комплекс засобів захисту;

АС – автоматизована система;

ІТС – інформаційно технологічний супровід;

КС – комп’ютерна система;

ТЗІ – технічний захист інформації.

ЗМІСТ

ВСТУП

Кожне підприємство, фірма, організація має свою організаційну структуру. Ця структура багатомірна і може бути складатися з кількох взаємопов’язаних і взаємозалежних підструктур, які можна розглядати як самостійні структури: структура управління виробництвом, кадрова структура, маркетингова, фінансово-економічна, інформаційна структури. Всі вони знаходяться в тісній взаємодії і саме їх сукупність і створює організаційну структуру підприємства. Одне з найважливіших місць у цій структурі займає інформаційна система.

Будь-яка система управління включає у себе інформаційну систему з різними інформаційними потоками у вигляді документів, розпоряджень, запитів, що обертаються усередині організації. Для стабільної роботи підприємства необхідно забезпечити стабільну роботу інформаційної системи. Один із критеріїв стабільності інформаційної системи – це інформаційна безпека. Тому система управління інформаційною безпекою (СУІБ) має бути невід’ємною частиною кожної системи управління.

Однією із найважливіших вимог забезпечення сталого функціонування будь-якого підприємства є надійність роботи інформаційної системи та зовнішніх інформаційних ресурсів в мережі Інтернет.

Відповідний заданим вимогам рівень інформаційної безпеки (ІБ) може бути досягнутий виключно за умови комплексного підходу, що містить у собі програмні, апаратні та організаційні міри захисту.

Доволі часто останніми нехтують, хоча вони є найбільш вагомими та в середньому повинні складати більше 60% від усіх заходів у цьому напрямку.

Політика безпеки інформації (ПБІ) є основою організаційних мір захисту інформації. Коректність її побудови однозначно впливає на ефективність заходів по забезпеченню ІБ. У загальних випадках, ПБІ визначається як система документованих управлінських рішень щодо забезпечення ІБ організації. В окремих випадках, під ПБІ звичайно розуміють локальний нормативний

документ, що визначає вимоги безпеки, систему заходів, або порядок дій, а також відповідальність співробітників організації і механізми контролю для забезпечення певної області ІБ.

Зазвичай, мотивами для створення політики безпеки є: додержання вимог чинного законодавства, виконання вимог керівництва організації, клієнтів або їх партнерів, підвищення конкурентоспроможності на ринку, підготовка до міжнародних сертифікацій, позбавлення зауважень аудиторів, економічна доцільність тощо. Стає очевидним, що створення ПБІ являється фундаментальною частиною побудови режиму інформаційної безпеки для організації ефективної роботи структури будь-якого типу та масштабів.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Напрям діяльності ТОВ «Охоронна фірма СТІНА» – надання фізичної охорони для торгівельних мереж. Підприємство веде свою діяльність з 2018 року. Офіс компанії знаходиться за адресою: місто Київ, вулиця Гната Хоткевича, будинок 12 офіс 177.

Режим роботи:

Робочі дні: понеділок – п’ятниця.

Час роботи: 09:00 – 18:00.

Перерва: з 12:00 до 13:00.

Штат працівників складає 18 осіб:

- Директор фірми – 1 людина;
- Заступник директора – 1 людина;
- Секретар – 1 людина;
- Менеджер з продажу – 1 людина;
- Бухгалтер – 1 людина;
- Системний адміністратор – 1 людина;
- Начальник охорони – 1 людина;
- Прибиральниця – 1 людина;
- Співробітник служби безпеки – 11 людей.

1.2 Обґрунтування необхідності створення КСЗІ

Згідно Закону України «Про захист інформації» в ІТС ТОВ «Охороннаа фірма СТІНА»оброблюється і зберігається інформація з обмеженим доступом.

Згідно Законів України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї

інформації визначаються власником інформації. Власник інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, якщо це не суперечить чинному законодавству.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» в ТОВ «Охоронна фірма СТІНА» АС відносяться до третього класу, оскільки представляє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Передача інформації здійснюється через незахищене середовище.

Комплексна система захисту інформації (КСЗІ) – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Комплекс технічного захисту інформації (КТЗІ) – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку ІзОД технічними каналами на об’єктах інформаційної діяльності.

Інформація з обмеженим доступом (ІзОД) – інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом.

Для забезпечення безпеки інформації під час її обробки в АС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу АС.

Комплекс засобів захисту (КЗЗ) – сукупність всіх програмно-апаратних засобів, задіяних під час реалізації політики безпеки.

Політика безпеки (ПБ) – набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації.

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» в ТОВ «Охоронна фірма СТІНА» циркулює

інформація з обмеженим доступом (персональні данні персоналу та клієнтів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником.

Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Тобто, перед створенням КСЗІ, треба визначити чи є на підприємстві інформація, яка підлягає захисту.

До організаційних заходів КСЗІ можна віднести:

1 Складання посадових інструкцій для користувачів та обслуговуючого персоналу;

2 Створення правил адміністрування системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікація користувачів;

3 Розробка порядку дій у випадках виявлення спроб НСД до ІС або виходу з ладу засобів захисту інформації;

4 Навчання користувачів правилам інформаційної безпеки.

Вибір інженерно-технічних заходів КСЗІ залежить від рівня захисту інформації. До них можна віднести:

1 Програмно-апаратні засоби захисту;

2 Розмежування потоків інформації між сегментами мережі;

3 Засоби шифрування і захисту від НСД;

4 СКУД та охоронно-пожежна сигналізація.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

1.3 Обстеження ОІД

На ситуаційному плані відображено положення об’єкту інформаційної діяльності відносно об’єктів місцевості.

Підприємство знаходиться у 10 поверховій офісній будівлі на 5 поверсі (Вул. Гната Хоткевича, 12, офіс 177). Контрольна зона обмежена стінами приміщення. Доступ на територію надається за перепустками та контролюється фізичною охороною в денний час та в нічний час, системою охоронної сигналізації в ночі.

На відстані 25 метрів від ОІД знаходиться проїзна частина.

На відстані 20 метрів від ОІД знаходиться житловий будинок 12.

На відстані 30 метрів від ОІД знаходиться житловий будинок 8.

На відстані 15 метрів від ОІД знаходиться трансформаторна підстанція ТП-14/5.

Фізичні характеристики будівлі і приміщень;

Загальна площа приміщення складає 95 м^2. Висота стін – 3 м. Товщина стін – 0.5 м. Підлога з кафелю, вікна - звичайний склопакет, двері в інші кімнати дерев’яні, вхідні двері в офіс броньовані. В приміщенні всього налічується 5 дверей і одні вхідні. Товщина стін кімнатки бухгалтера 0.3 м. Стіни залізобетонні. Перегородки з цегли. Є система кондиціонування, звичайна, загальна.

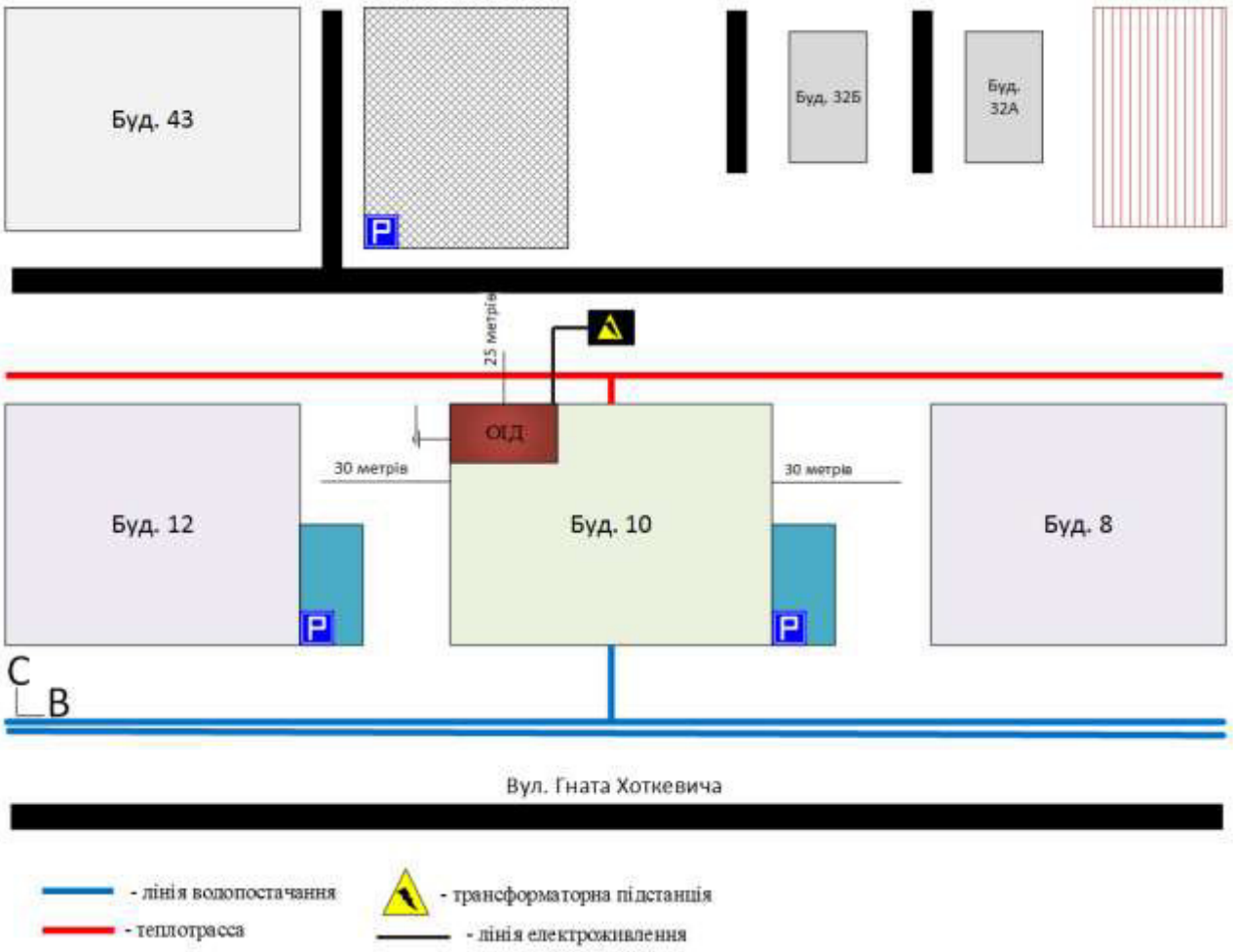

Рисунок 1.1 – Ситуаційний план

Таблиця 1.1 – Система комунікацій, життєзабезпечення та зв’язку.

Система комунікацій	**Спосіб підключення**
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ.
Електроживлення	Підключено до трансформаторної підстанції, котра обслуговує сторонніх споживачів і виходить за межі КЗ.
Система водопостачання	Підключена до міського водоканалу, котрий виходить за межі КЗ
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ.
Заземлення	Всі прилади, комп’ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.

Продовження таблиці 1.1

Корпоративний фіксований телефонний зв'язок	Мобільна лінія «Київстар». На всіх співробітників виділені мобільні номера.
Корпоративний фіксований інтернет	Підключена до Інтернет-провайдеру «Київстар».
Система вентиляції	Приточно-витяжна, Спліт система.
Система сигналізації	Складається з датчиків відкриття (магнітно-контактний датчик), датчиків руху (пасивні інфрачервоні) та системи кабелів.
Протипожежна сигналізація	Складається з системи оповіщувачів та датчиків, дані з яких обробляються протипожежним прийомно-контрольним пристроєм, що знаходиться на пості охорони, та підключений до міської системи оповіщення пожежної охорони.
Кабелі компютерної мережі	Кабель локальної мережі комп’ютерів являє собою неекранована вита пара категорії 5е.

Рисунок 1.2 – Генеральний план

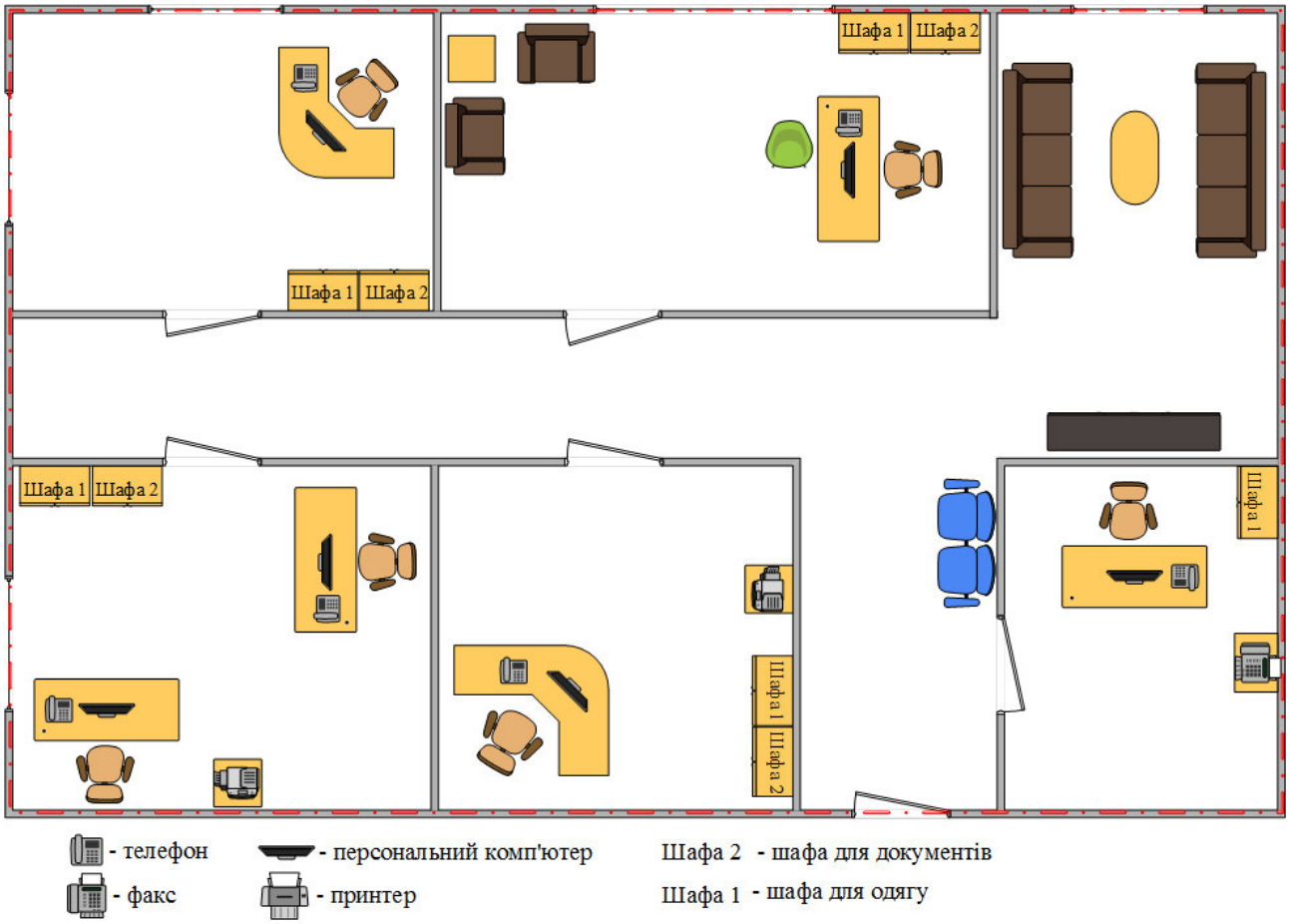

Рисунок 1.3 – Контур контрольної зони

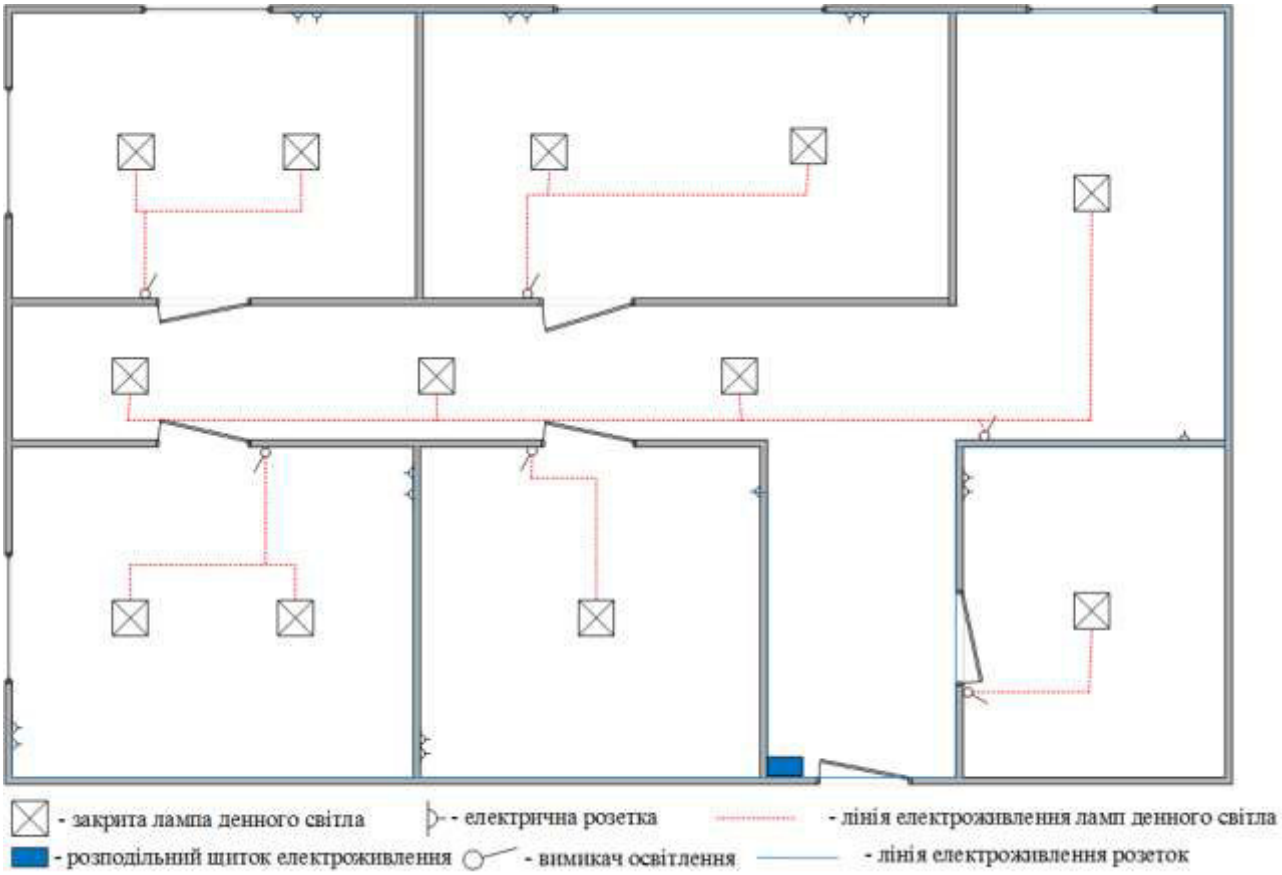

Рисунок1.4 – Система електроживлення

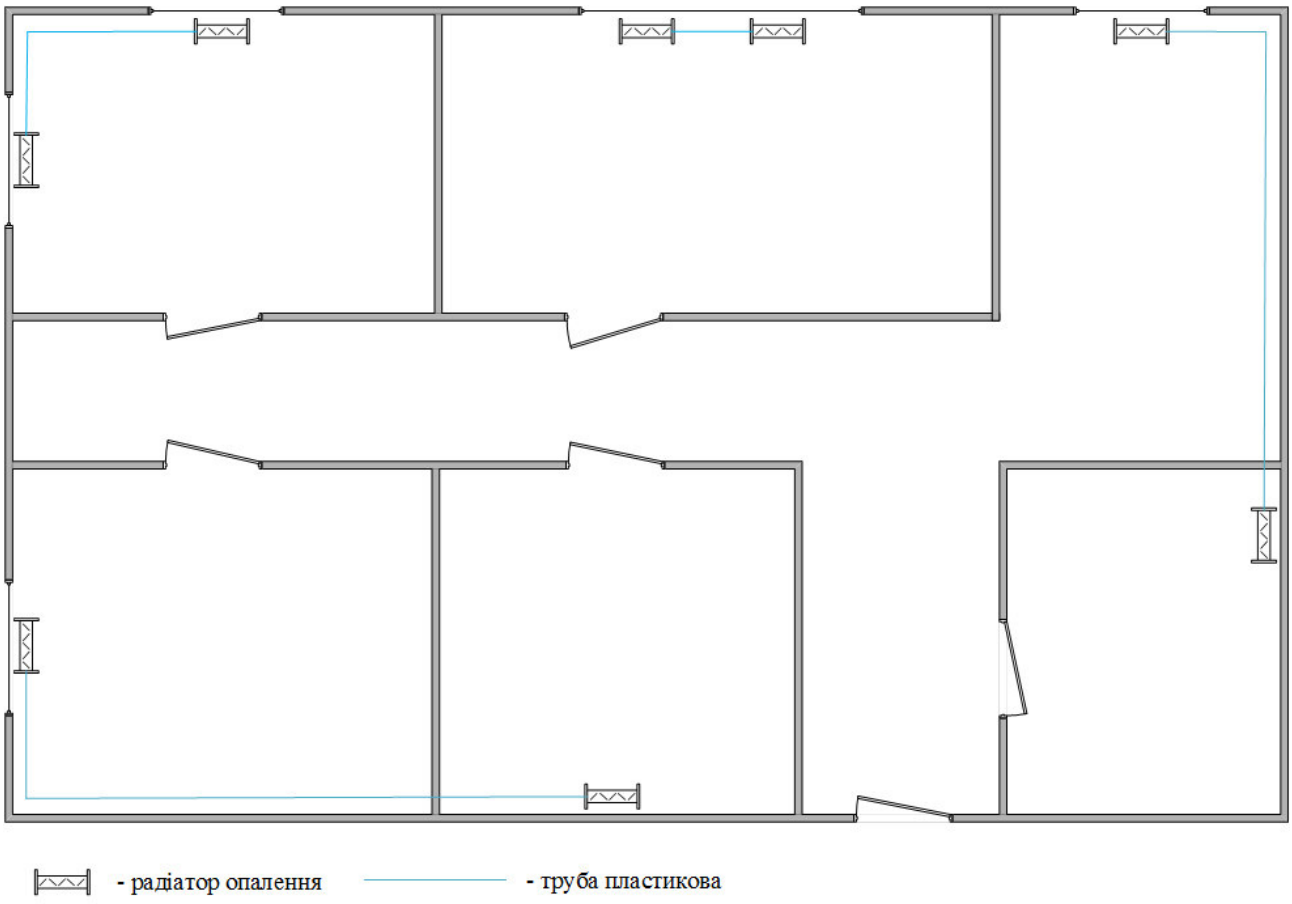

Рисунок 1.5 – Система опалення

Рисунок 1.6 – Система телефонного зв’язку

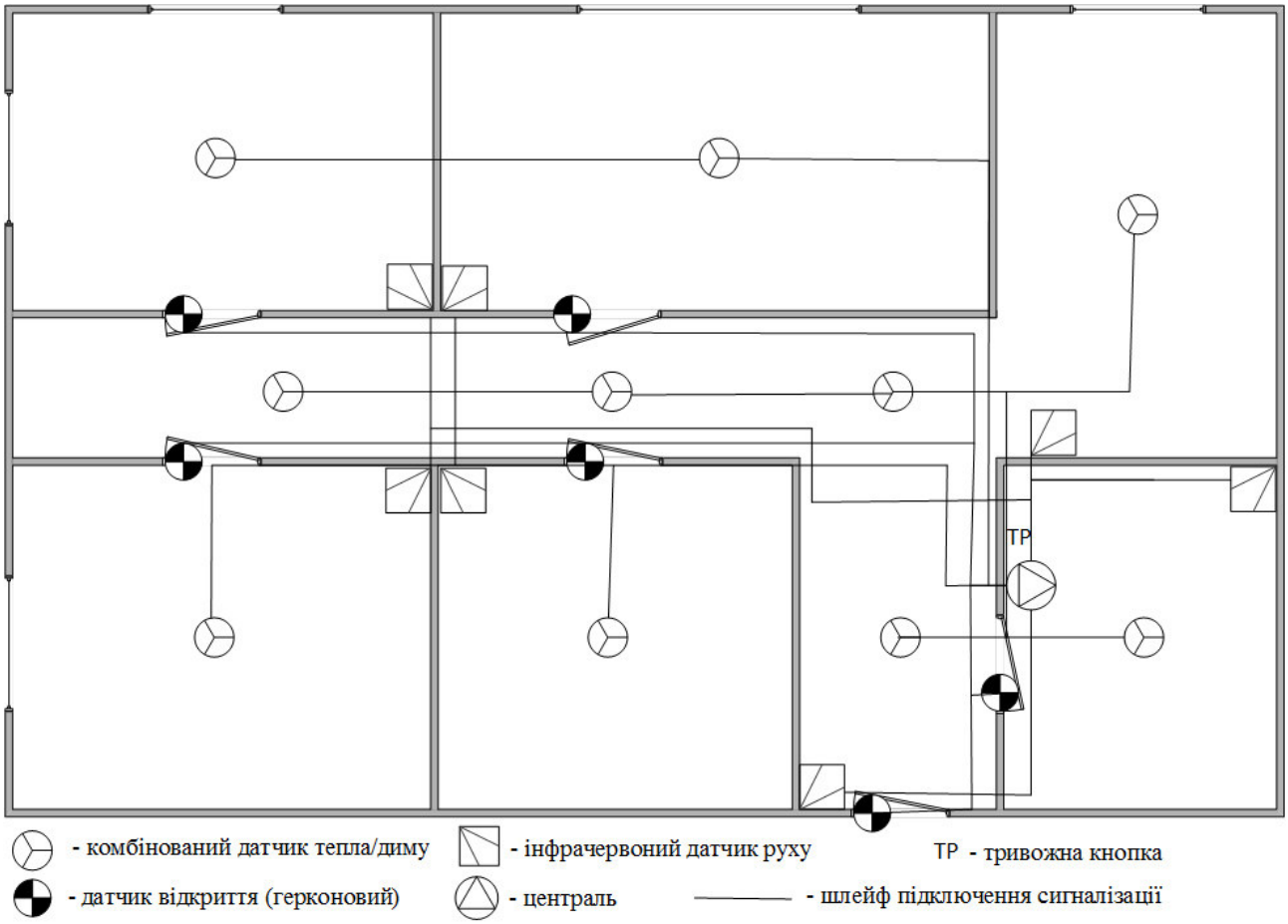

Рисунок 1.7 – Система пожежної та охоронної сигналізації

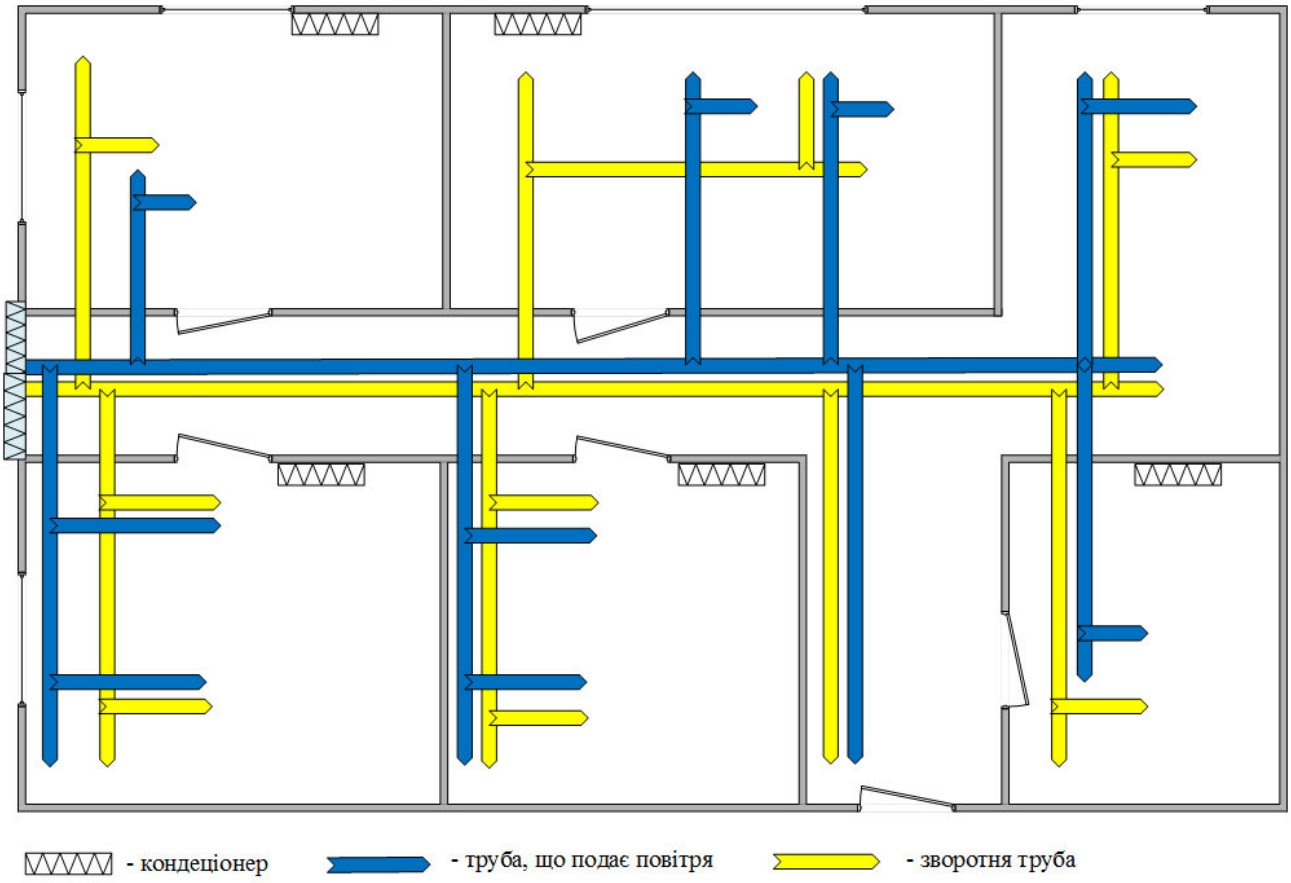

Рисунок 1.8 – Система кондиціонування

На досліджуваному ОІД циркулює інформація з обмеженим доступом: конфіденційна.

В мережі відділу кожному комп’ютеру присвоєне мережеве ім’я.

Вихід комп’ютерів до мережі Інтернет забезпечується за допомогою маршрутизатора підключеного до каналу «КИЇВСТАР».

Цінна для об’єкту інформація дублюється на комп’ютерах співробітників з подібними правами доступу до неї.

Склад обчислюваної системи вказано у таблиці 1.2 та на рисунку 1.9

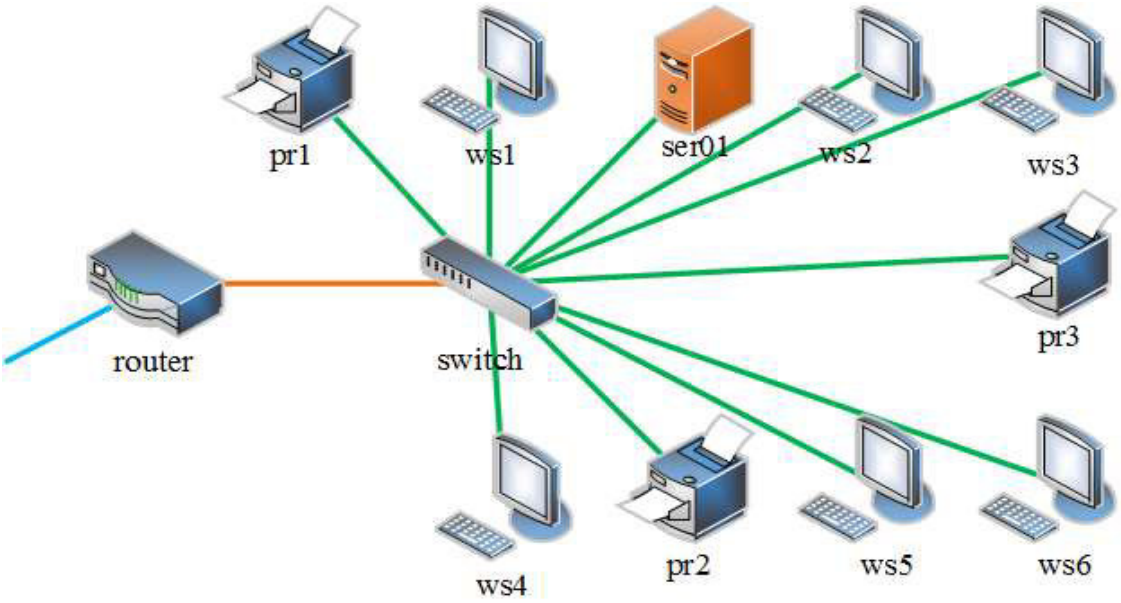

Рисунок 1.9 – Комп’ютерна мережа

Таблиця 1.2 – Склад та характеристики обчислюваної системи

Назва	**Характеристика**	**Умовні позначення**	**Кількість**
Робоча станція	Intel Core i5-7400 (3.0 ГГц) / RAM 8 ГБ / HDD 500 ГБ / LAN / Windows 10 Pro 64-bit / Samsung S22F350F / Logitech K120 USB / Мышь Logitech M90 USB	ws1-ws6	6
Сервер	HPE ProLiant ML10 Gen9: Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц) / 8 ГБ / 2 x 1 ТБ (SATA 3, 7200 об/мин) HPE LFF	ser01	1
Принтери	HP LaserJet Pro M130nw (G3Q58A)	pr1-pr3	3
Комутатор	D-Link DES-1100-16 / 16 x Fast Ethernet (10/100 Мбит/с) / Керований	switch	1
Маршрутизатор	D-Link DSR-250 / 1 x WAN 10/100/1000 Мбит/с / 8 x LAN 10/100/1000 Мбит/с / 1 порт USB 2.0 / Консоль RJ-45	router	1

Таблиця 1.3 – Встановлене програмне забезпечення на робочі станції та сервері

Розміщення	**Тип**	**Назва**
Сервер БД	Операційна система	Microsoft Windows Server 2016 R2
	ПЗ для роботи з документами	Microsoft Office 2016
	ПЗ для автоматизації бухгалтерського обліку	1С: Бухгалтерія 8.1
	Антивірус, міжмережевий екран	ESET Endpoint Security
Робочі станції	Операційна система	Windows 10 Pro 64-bit
	ПЗ для роботи з документами	Microsoft Office 2016
	Веб-браузер	Google Chrome 67.0.3396.62
	ПЗ для автоматизації бухгалтерського обліку	1С: Бухгалтерія 8.1 клієнт
	Антивірус, міжмережевий екран	ESET Endpoint Security

Всі документи створюються відповідними працівниками на своїх робочих станціях за допомогою встановленого ПЗ та роздруковуються на принтерах чи розмножуються. Електрона копія зберігається або на робочий станції працівника або в спеціально відведеному місці (папка на диску) на сервері для документів, роздрукований паперовий варіант зберігається в шафі або в сейфі. Після втрати необхідності в документі він знищується.

Таблиця 1.4 – Класифікація інформації

№	**Вид інформації**	**Режим доступу**	**Вид зберігання**	**Вимоги**
1	Особисті дані персоналу	ІзОД	Паперовий та електронний	К, Ц, Д
2	БД підприємства, відділу	ІзОД	Паперовий та електронний	К, Ц, Д
3	Договори, укладені з клієнтами	ІзОД	Паперовий та електронний	К, Ц, Д
4	Інформація бухгалтерської звітності	ІзОД	Паперовий та електронний	К, Ц, Д
5	Інформація про стан мережі, її компонентів	ІзОД	Електронний	К, Ц, Д
6	Інформація про засоби захисту інформації	ІзОД	Паперовий та електронний	К, Ц, Д
7	Трудові договори	ІзОД	Паперовий	К, Ц, Д
8	Інформація про послуги та їх вартість	Відкрита	Паперовий та електронний	Ц, Д
9	Інформація про діяльність підприємства	Відкрита	Паперовий та електронний	Ц, Д
10	Статутні документи підприємства	Відкрита	Паперовий та електронний	Ц, Д

К – вимоги до конфіденційності;

Ц – вимоги до цілісності;

Д – вимоги до доступності.

В таблиці 1.5 вказано які користувачі можуть здійснювати керування інформаціє

Таблиця 1.5 – Матриця доступу

Посада	Директор	Зас. Директора	Секретар	Системний адміністратор	Бухгалтер	Менеджер з продажу	Начальник охорони	Співробітник служби безпеки
1	C,R,W,D	C,R,W,D	R	R	C,R,W,D	-	R	-
2	C,R,W,D	C,R,W,D	R	-	C,R,W	-	-	-
3	C,R,W,D	C,R,W,D	R	-	C,R,W	R,W	R	-
4	R,W	R,W	-	-	C,R,W,D	-	-	-
5	R,W	R,W	-	C,R,W,D	-	-	-	-
6	R,W	R,W	-	C,R,W,D	-	-	-	-
7	R,W,D	R,W,D	R	R	C,R,W,D	-	R	-
8	C,R,W,D	C,R,W,D	R	-	R,W	R	R	R
9	R,W	R,W	R	R	R	R	R	R
10	R,W	R,W	R	R	R	R	R	R

C – create (право на створювання); R – read (право на зчитування); W – write (право на редагування); D – delete (право на видалення).

1.4 Аналіз загроз інформації, що циркулює на ОІД

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Загрози інформаційної безпеки класифікуються за низькою ознак:

– за складовими інформаційної безпеки;

– за компонентами інформаційних систем, на які загрози націлені;

– за характером впливу;

– за розміщенням джерела загроз.

Розглянемо класифікацію загроз інформаційної безпеки за її складовими. Класифікація загроз інформаційної безпеки за її складовими полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної безпеки, як цілісність, доступність, конфіденційність. Усі загрози, що класифікуються за іншими ознаками можуть впливати на усі складові інформаційної безпеки.

Також загрози інформаційної безпеки можуть бути розділені за компонентами інформаційних систем, на які вони націлені. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які загрози націлені полягає у визначенні загроз (загрози), які безпосередньо направлені на такі складові інформаційної системи, як інформація, що обробляється в обчислювальної системі, обчислювальна система, програмне забезпечення, апаратура, персонал та інші.

В якості прикладів загроз компонентам інформаційних систем, що суттєво впливають на стан захищеності інформації, можна навести такі:

– зміна архітектури системи;

– зміна складу та/або можливостей апаратних і програмних засобів;

– підключення до мережі (особливо глобальної);

– відмінності в категорії та/або кваліфікації персоналу.

Загрози інформаційної безпеки за характером впливу класифікують, як випадкові та навмисні дії природного або техногенного характеру.

Випадкові загрози – це загрози, які не пов’язані з умисними діями зловмисників та реалізуються у випадкові моменти часу. Випадкові загрози поділяють на загрози від аварій та стихійних лих, збоїв та відмов технічних засобів, помилок при розробці елементів інформаційної системи, алгоритмічні та програмні помилки, помилки користувачів чи обслуговуючого персоналу та інші. Реалізація цих загроз веде до найбільшої втрати інформації. Це – знищення, порушення цілісності, доступності, інколи – конфіденційності інформації.

Навмисні загрози – це цілеспрямовані дії зловмисника. Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, недостатньо вивчений.

Навмисні загрози поділяють на:

– «спеціальні впливи»;

– несанкціонований доступ до інформації;

– використання технічних каналів витоку інформації;

– несанкціоновану зміну структури та інші.

Спроба реалізації будь якої навмисної загрози по відношенню до об’єкту інформаційної діяльності підпадає під дію відповідних статей Карного кодексу України.

«Спеціальні впливи». Загрози інформаційної безпеці від традиційних «спеціальних впливів» до цього часу залишаються актуальними. Частіше за все їх використовують для отримання інформації про систему захисту інформації або її знищення з метою подальшого проникнення до інформаційної системи.

Методами «спеціальних впливів» є: підслуховування, візуальне спостереження, викрадення документів або носіїв інформації, викрадення програм або атрибутів системи захисту інформації, підкуп або шантаж співробітників, сбір та аналіз відходів машинних носіїв інформації, підпалення та інші.

Розрізняють два класи загроз інформації за розміщенням їх джерела в середині інформаційної системи, або поза неї.

Найбільш небезпечною загрозою вважається внутрішня загроза, джерелом якої є співробітники установи – користувачі інформаційної системи. Серед користувачів є специфічна категорія – керівництво. Часто, керівники вимагають собі підвищені привілеї в системі, а також не визнають щодо себе жодних обмежень. До того ж, адміністратори системи формально підпорядковані керівництву, а не навпаки.

Потенційні можливості легального користувача в ІКС значно більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Користувач має багато інформації про систему, а іншу інформацію може порівняно легко отримати (когось спитати, підслухати, «неформально» проконсультуватись – йому це значно простіше, ніж будь-якій сторонній особі). Користувач, як правило, незадоволений обмеженнями своїх прав у системі. Користувач цікавиться інформаційними технологіями і бажає перевірити свої досягнення на практиці. Часто користувач не дуже кваліфікований, і все, що він буде робити, фактично зведеться до методу спроб і помилок.

Модель загроз (model of threats) – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Носіями загроз безпеки інформації є джерела загроз. У якості джерел загроз можуть виступати як суб’єкти (особистість), так і об’єктивні прояви. Причому, джерела загроз можуть перебувати як усередині організації, що захищається, – внутрішні джерела, так і поза неї – зовнішні джерела. Розподіл джерел на суб’єктивні й об’єктивні виправдане виходячи із приводу провини або ризику збитку інформації. А розподіл на внутрішні й зовнішні джерела виправдане тому, що для однієї й тієї ж загрози методи парирування для зовнішніх і внутрішніх джерел можу бути різними.

Всі джерела загроз безпеки інформації можна розділити на три основні групи:

– обумовлені діями суб’єкта (антропогенні джерела загроз);

– обумовлені технічними засобами (техногенні джерела загроз);

– обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеки інформації виступають суб’єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорить про заподіяння збитку. Ця група найбільш велика й становить найбільший інтерес із погляду організації захисту, тому що дії суб’єкта завжди можна оцінити, спрогнозувати й вжити адекватні заходи. Методи протидії в цьому випадку керовані й прямо залежать від волі організаторів захисту інформації.

У якості антропогенного джерела загроз можна розглядати суб’єкт, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об’єкту, що захищається. Техногенні виникають внаслідок використання техніки. Загрози, пов’язані з втратою або псуванням інформації внаслідок виходу з ладу обладнання важко спрогнозувати і попередити.

Стихійні лиха – це група джерел, яка представляє обставини, що мають непереборну силу и не піддаються попередженню. Найчастіше сюди відносять стихійні лиха та природні катаклізми, техногенні катастрофи, пожежі. Вони не піддаються прогнозуванню, тому заходи захисту від їх наслідків повинні виконуватися постійно.

Суб’єкти (джерела), дії яких можуть привести до порушення безпеки інформації, можуть бути як зовнішні, так і внутрішні. Зовнішні джерела можуть бути випадковими або навмисними й мати різний рівень кваліфікації.

Внутрішні суб’єкти (джерела), як правило, являють собою висококваліфікованих фахівців в області розробки й експлуатації програмного забезпечення й технічних засобів, знайомих зі специфікою розв’язуваних задач, структурою й основними функціями й принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного устаткування й технічних засобів мережі.

При розгляданні моделі загроз, також слід приділити увагу дестабілізуючим факторам. Дестабілізуючі фактори (ДФ) – це такі явища чи події, що можуть з’являтися на будь-якому етапі життєвого циклу АС і наслідком яких можуть бути загрози інформації. У продовження життєвого циклу АС може виникати багато ДФ всілякої природи.

Тому, на основі аналізу архітектури, технології й умов функціонування АС і всіх можливих у принципі ДФ зручно ввести поняття типу ДФ, що дозволяє класифікувати ДФ за способами їхньої реалізації. Вважаючи, що ця класифікація ДФ є вичерпною, виділимо наступні типи ДФ:

– кількісна недостатність – фізична недостатність компонентів АС для забезпечення необхідного рівня захищеності оброблюваної інформації;

– якісна недостатність – недосконаліть конструкції чи організації компонентів АС, внаслідок чого не забезпечується необхідний рівень захищеності оброблюваної інформації;

– відмова елементів АС – порушення працездатності елементів, що

– збій елементів АС – тимчасове порушення працездатності елементів, що призводить до неправильного виконання ними в цей момент своїх функцій;

– помилки елементів АС – неправильне (одноразове чи систематичне) виконання елементами своїх функцій внаслідок специфічного (постійного і/або тимчасового) їхнього стану;

– стихійні лиха – випадково виникаючі неконтрольовані явища, що

– призводять до фізичних руйнувань;

В таблиці 2.6 представлено аналіз загроз, вона допомагає виявити через які загрози, джерела загроз можуть нести найбільшу небезпеку. Така таблиця в подальшому допоможе розробити заходи для мінімізації цих загроз.

$(K1)_f$ – фатальність, визначає міра впливу уразливості на неможливість усунення наслідків реалізації загрози. Для об’єктивних вразливостей це

інформативність – здатність вразливості повністю (без спотворень) передати корисний інформаційний сигнал.

$(К2)_f$ – доступність, визначає зручність (можливість) використання вразливості джерелом загроз (багато габаритні розміри, складність, вартість необхідних засобів, можливість використання не спеціалізованої апаратури).

$(К3)_f$ – кількість, визначає кількість елементів об'єкту, яким характерна та або інша вразливість. $(К_{неб})_{f_.} = \frac{К_1 \times К_2 \times К_3}{125}$.

Таблиця 1.6 – Аналіз загроз

Джерело загроз	**Загроза**	**К**	**Д**	**Ц**	**$К_1$**	**$К_2$**	**$К_3$**	**$К_{неб}$**
1	2	3	4	5	6	7	8	9
Антропогенні, зовнішні								
Кримінальні структури	Крадіжка (копіювання) інформації	+	+	+	3	1	3	0,072
	Знищення інформації	+	+	+	3	1	2	0,048
	Змінення інформації	+	+	+	1	2	2	0,032
	Порушення доступності (блокування) інформації	+	+	+	1	1	2	0,016
	Заперечення достовірності інформації	+	+	+	1	1	2	0,016
	Нав'язування помилкової інформації	+	+	+	1	1	2	0,016
Хакери	Крадіжка (копіювання) інформації	+	+	+	3	3	2	0,144
	Знищення інформації	+	+	+	3	3	3	0,216
	Змінення інформації	+	+	+	3	3	3	0,216
	Порушення доступності (блокування) інформації	+	+	+	3	2	2	0,096
	Заперечення достовірності інформації	+	+	+	4	2	3	0,192
	Нав'язування помилкової інформації	+	+	+	3	3	3	0,216

Продовження таблиці 1.6

Конкуренти	Крадіжка (копіювання) інформації	+	+	+	2	4	2	0,128
	Знищення інформації	+	+	+	2	4	2	0,128
	Змінення інформації	+	+	+	2	3	2	0,096
	Порушення доступності (блокування) інформації	+	+	+	1	4	2	0,064
	Заперечення достовірності інформації	+	+	+	2	4	1	0,064
	Нав'язування помилкової інформації	+	+	+	1	3	2	0,048
Відвідувачі	Крадіжка (копіювання) інформації	+	+	+	3	2	2	0,096
	Знищення інформації	+	+	+	3	2	2	0,096
	Змінення інформації	+	+	+	3	2	2	0,096
	Порушення доступності (блокування)	+	+	+	2	2	2	0,064
	Заперечення достовірності інформації	+	+	+	3	1	2	0,048
	Нав'язування помилкової інформації	+	+	+	2	1	2	0,032
Будь які особи, що знаходяться за межами КЗ	Крадіжка (копіювання) інформації	+	+	+	1	1	2	0,016
	Знищення інформації	+	+	+	1	1	2	0,016
	Змінення інформації	+	+	+	1	1	2	0,016
	Порушення доступності (блокування) інформації	+	+	+	1	1	2	0,016
	Заперечення достовірності інформації	+	+	+	1	1	1	0,008
	Нав'язування помилкової інформації	+	+	+	1	2	2	0,032

Продовження таблиці 1.6

Антропогенні, внутрішні (авторизовані користувачі)								
Директор фірми	Крадіжка (копіювання) інформації	+	+	+	5	3	4	0,48
	Знищення інформації	+	+	+	5	4	4	0,64
	Змінення інформації	+	+	+	5	3	4	0,48
	Порушення доступності (блокування) інформації	+	+	+	5	3	4	0,48
Основний персонал (користувачі мережі)	Крадіжка (копіювання) інформації	+	+	+	4	3	3	0,288
	Знищення інформації	+	+	+	4	3	4	0,384
	Змінення інформації	+	+	+	4	3	4	0,384
	Порушення доступності (блокування)	+	+	+	4	2	3	0,192
	Заперечення достовірності інформації	+	+	+	3	3	3	0,216
	Нав’язування помилкової інформації	+	+	+	4	2	3	0,192
Системний адміністатор	Крадіжка (копіювання) інформації	+	+	+	5	5	4	0,8
	Знищення інформації	+	+	+	5	5	4	0,8
	Змінення інформації	+	+	+	5	5	4	0,8
	Порушення доступності (блокування)	+	+	+	5	5	4	0,8
	Заперечення достовірності інформації	+	+	+	5	4	4	0,64
	Нав’язування помилкової інформації	+	+	+	5	5	4	0,8

Продовження таблиці 1.6

Антропогенні, внутрішні (персонал, який не є авторизованими користувачами)								
Прибиральниця	Крадіжка (копіювання) інформації	+	+	-	3	1	2	0,048
	Знищення інформації	+	+	-	3	1	2	0,048
	Змінення інформації	+	+	-	4	1	1	0,032
	Порушення доступності (блокування) інформації	+	+	-	3	2	2	0,096
	Заперечення достовірності інформації	+	+	-	4	1	2	0,064
	Нав'язування помилкової інформації	+	+	-	4	2	2	0,128
Техногенні, зовнішні								
Засоби зв'язку	Крадіжка (копіювання) інформації	+	-	+	2	2	2	0,064
	Знищення інформації	+	-	+	2	1	2	0,032
	Змінення інформації	+	-	+	2	2	1	0,032
	Порушення доступності (блокування) інформації	+	-	+	3	2	2	0,096
	Заперечення достовірності інформації	+	-	+	2	1	1	0,016
	Нав'язування помилкової інформації	+	-	+	2	2	2	0,064
Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення)	Крадіжка (копіювання) інформації	+	-	+	3	2	3	0,144
	Знищення інформації	+	-	+	3	2	2	0,096
	Змінення інформації	+	-	+	3	1	2	0,048
	Порушення доступності (блокування) інформації	+	-	+	1	2	2	0,032
	Заперечення достовірності інформації	+	-	+	3	1	2	0,048

Продовження таблиці 1.6

Техногенні, внутрішні								
Неякісне апаратне забезпечення	Крадіжка (копіювання) інформації	+	+	+	4	2	2	0,128
	Знищення інформації	+	+	+	4	3	2	0,192
	Змінення інформації	+	+	+	4	2	3	0,192
	Порушення доступності (блокування) інформації	+	+	+	4	2	3	0,192
	Заперечення достовірності інформації	+	+	+	4	2	1	0,064
	Нав’язування помилкової інформації	+	+	+	4	2	2	0,128
	Крадіжка (копіювання) інформації	+	+	+	4	2	2	0,128
Стихійні								
Пожежі		-	+	-	2	2	2	0,064
Землетруси		-	+	-	2	1	1	0,016
Підтоплення		-	+	-	1	1	2	0,016
Урагани		-	+	-	1	1	2	0,016
Різні непередбачені обставини		-	+	-	2	1	2	0,032
Інші форс-мажорні обставини		-	+	-	2	1	2	0,032

Розглянемо наступну таблицю 1.7, враховуючи дані таблиці 1.6, виділимо загрози, які найбільше піддаються впливу зі сторони джерел загроз.

Таблиця 1.7 – Загрози, що найбільше піддаються впливу

Джерело загроз	**Загроза**	**$К_{неб}$**
Антропогенні, зовнішні		
Кримінальні структури	Крадіжка (копіювання) інформації	0,072
Хакери	Знищення інформації	0,216
	Змінення інформації	0,216
	Нав’язування помилкової інформації	0,21

		6

Продовження таблиці 1.7

Відвідувачі	Крадіжка (копіювання) інформації	0,096
	Знищення інформації	0,096
	Змінення інформації	0,096
Будь які особи, що знаходяться за межами КЗ	Нав’язування помилкової інформації	0,032
Антропогенні, внутрішні (авторизовані користувачі)		
Директор фірми	Знищення інформації	0,64
Основний персонал (користувачі мережі)	Знищення інформації	0,384
	Змінення інформації	0,384
Системний адміністатор	Крадіжка (копіювання) інформації	0,8
	Знищення інформації	0,8
	Змінення інформації	0,8
	Порушення доступності (блокування)	0,8
	Нав’язування помилкової інформації	0,8
Антропогенні, внутрішні (персонал, який не є авторизованими користувачами)		
Прибиральниця	Нав’язування помилкової інформації	0,128
Техногенні, зовнішні		
Засоби зв’язку	Порушення доступності (блокування) інформації	0,096
Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення)	Знищення інформації	0,096
Техногенні, внутрішні		
Неякісне апаратне забезпечення / Неякісне програмне забезпечення	Знищення інформації	0,192
	Змінення інформації	0,192
	Порушення доступності (блокування) інформації	0,192
Стихійні		

Пожежі	0,064

Модель порушника

Модель порушника (user violator model) – абстрактний формалізований або неформалізований опис порушника.

Порушник (user violator) – користувач, який здійснює НСД до інформації. Оскільки під порушником розуміється людина, то цілком зрозуміло, що створення його формалізованої моделі дуже складна задача. Тому, звичайно, мова може йти тільки про неформальну або описову модель порушника.

Порушник – це особа, яка може отримати доступ до роботи з включеними в склад АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він переслідує);

– припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що у своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему.

Звичайно розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи: зовнішні і внутрішні порушники.

Зовнішні порушники включають:

– добре озброєну й оснащену силову групу, що діє зовні швидко і напролом;

– поодинокий порушник, що не має допуску на об’єкт і намагається діяти потайки й обережно, так як він усвідомлює, що сили реагування мають перед ним переваги.

Серед потенціальних внутрішніх порушників можна відзначити:

– допоміжний персонал об’єкту, що допущений на об’єкт, але не допущений до життєво важливого центру АС;

– основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

– співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Категорія осіб, до якої може належати порушник:

– внутрішні порушники;

– користувачі;

– інженерний склад;

– співробітники відділів, що супроводжують ПЗ;

– технічний персонал, що обслуговує будинок;

– співробітники служби безпеки;

– керівники;

– зовнішні порушники.

Мета порушника:

– отримання необхідної інформації;

– отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в АС:

– запуск фіксованого набору задач (програм);

– створення і запуск власних програмних засобів;

– керування функціонуванням і внесення змін у конфігурацію системи;

– підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

– апаратні засоби;

– програмні засоби;

– спеціальні засоби.

Кваліфікація порушника:

для аналізу загроз завжди приймається висока кваліфікація.

Таблиця 1.8 – Модель порушника

Джерело загрози	**Загрози**			**Інформація, яка зазнає впливу від джерел загроз**
	К	**Д**	**Ц**	
Внутрішні				
директор фірми	+	+	+	1,2,3,5,6,7,8,9,10
секретар	+	+	+	1,2,3,7,8,9,10
заступник директора	+	+	+	1,2,3,5,6,7,8,9,10
начальник охорони	+	+	+	1,2,3,7,8,9,10
менеджер з продажу	+	+	+	1,2,3,7,8,9,10
бухгалтер	+	+	+	1,2,3,4,7,8,9,10
системний адміністратор	+	+	+	1,5,6,7
співробітник служби безпеки	+	+	-	2,3,8
прибиральниця	+	+	-	2,3,8
Зовнішні				
кримінальні структури	+	+	+	1,2,3,4,5,6,7,8
хакери	+	+	+	1,2,3,4,5,6,7,8
конкуренти	+	+	+	2,3,4,8

відвідувачі	+	+	+	1,2,3,4,7,8
будь які особи, що знаходяться за межами КЗ	+	+	+	1,2,3,4,7,8

В таблиці 1.9, за результатами аналіза загроз та визначення порушників, виділено найбільш значущі джерела загроз ІБ.

Таблиця 1.9 – Загрози, що найбільше піддаються впливу

Джерело загроз	**Небезпека**
Антропогенні	
Системний адміністатор	0,8
Директор фірми	0,64
Основний персонал (користувачі мережі)	0,384
Хакери	0,216
Конкуренти	0,128
Прибиральниця	0,128
Відвідувачі	0,096
Кримінальні структури	0,072
Будь які особи, що знаходяться за межами КЗ	0,032
Техногінні	
Засоби зв’язку	0,096
Мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення)	0,096
Неякісне апаратне забезпечення / Неякісне програмне забезпечення	0,192
Стихійні	
Пожежі	0,064
Землетруси	0,016
Підтоплення	0,016
Урагани	0,016

Різні непередбачені обставини	0,032
Інші форс-мажорні обставини	0,032

Виходячи з таблиці 1.9, серед антропогенних джерел загроз найбільшу небезпеку становить системний адміністратор, він має коефіцієнт 0,8 та директор, у якого коефіцієнт становить 0,64. Серед техногенних джерел загроз, найбільший коефіцієнт отримали такі джерела загроз, як неякісне апаратне забезпечення / неякісне програмне забезпечення, у них коефіцієнт становить 0,192. Та серед стихійних джерел загроз, найбільші коефіцієнт небезпеки 0,064 отримала пожежа.

Аналіз ризиків

Ризик (risk) – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в ІТС.

При ідентифікації загроз з об’єктами захисту встановлюється відповідність моделі загроз і об’єктів захисту, тобто складається матриця загрози/компоненти (ресурси) ІТС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс ІТС. У процесі упорядкування матриці може уточнюватися список загроз і об’єктів захисту, внаслідок чого коригуватись модель загроз.

Під час оцінки ризиків повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій).

Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації.

На практиці для більшості загроз неможливо одержати достатньо об’єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Спочатку потрібно оцінити наслідки (цінність активів) у визначеному масштабі (0-4), кожного активу, якому загрожують (стовпчик «b» в таблиці 2.10).

Наступним кроком потрібно оцінити імовірність входження загрози у визначеному масштабі (0-4), кожної загрози (стовпчик «c» в таблиці 2.10).

Далі необхідно підрахувати міру ризику, множенням (b x c). Загрози можуть бути ранжовані в порядку їх зв’язаної міри ризику.

В таблиці 1.10 використано 1, як найнижчий наслідок і найнижчу імовірність загрози.

Таблиця 1.10 – Аналіз ризиків

Загрози	**Наслідки (b)**	**Імовірність поширення загроз (c)**	**Міра ризику (d)**	**Ранжування загрози (e)**
Крадіжка (копіювання) інформації	2	3	6	1
Знищення інформації	3	2	6	1
Змінення інформації	2	2	4	2
Порушення доступності (блокування) інформації	2	2	4	2
Заперечення достовірності інформації	1	2	2	3
Нав’язування помилкової інформації	1	1	1	3

Для стовпців «b» і «c»:

1 – низький; 2 – середній; 3 – високий.

Для стовпця «e»:

1: 5 – 6 – високий;

2: 3 – 4 – середній;

3: 1 – 2 – низький.

Згідно таблиці 1.10, найбільші значення важливості отримали загрози «Крадіжка (копіювання) інформації» та «Знищення інформації» – 1 (ранжування здійснювалося в порядку пріоритетності, тобто 1 є найважливіше значення). Тому вони несуть в собі найбільший ризик для підприємства.

Профіль захищеності

Функціональний профіль захищеності складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Після проведення обстеження ТОВ «Охоронна фірма СТІНА» була вивчена його інформаційна діяльність, були вивчені об'єкти захисту – ІзОД, виявлені загрози, зроблений їх аналіз та побудована окрема модель загроз.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Для стандартних функціональних профілів захищеності не вимагається ні зв'язаної з ними політики безпеки, ні рівня гарантій, хоч їх наявність і допускається в разі необхідності. Політика безпеки КС, що реалізує певний стандартний профіль, має бути «успадкована» з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в АС. Так, один і той же профіль захищеності може використовуватись для опису функціональних вимог з захисту оброблюваної інформації і для ОС, і для

СУБД, в той час, як їх політика безпеки, зокрема визначення об’єктів, буде різною.

Згідно з нормативними документами НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-005-99 треба визначити критерії захищеності даної АС.

На досліджуваному ОІД АС належить до третього класу, а вимоги до захисту інформації (конфіденційність, цілісність та доступність), то обраний профіль має вигляд:

3.КЦД.1 = {КД-2, КО-1, КВ-1,

ЦД-1, ЦО-1, ЦВ-1,

ДР-1, ДВ-1,

НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

Аналіз виконання послуг профіля захищеності

Розглянемо таблицю 2.11 в якій наведені критерії, що виконуються.

Таблиця 1.11 – Критерії, що виконуються

Критерії	**Пояснення**
КД-2. Базова довірча конфіденційність	Є розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта; адміністратор може вказати, які конкретні користувачі мають право одержувати інформацію від об’єкта. Виконується, так як є множина об’єктів КС.
КО-1. Повторне використання об’єктів	Виконуються, так як інформація, що знаходиться на звільненому об’єкті не стає недосяжною для інших користувачів.
КВ-1. Мінімальна конфіденційність при обміні	Виконується, якщо відомо, що при обміні інформацією використовуються захищені (зашифровані) лінії передачі.
ЦД-1. Мінімальна довірча цілісність	Виконується, так як користувач сам ранжує інформацію.
ЦО-1. Обмежений відкат	Виконується тому, що користувачу дозволяється відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об’єктом за певний проміжок часу.
ЦВ-1. Мінімальна	Виконується автоматично в певних механізмах

цілісність при обміні	системи (наприклад: оновлення ОС, антивірусу).

Продовження таблиці 1.11

ДР-1. Квоти	Виконується, так як користувач з правами адміністратора контролює кількість виділених ресурсів.
ДВ-1. Ручне відновлення	Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. Виконується автоматично системними засобами до моменту останнього оновлення.
НР-2. Захищений журнал	Виконується, так як для доступу до журналу треба мати права адміністратор, щоб потрапити до реєстру.
НК-1. Однонаправлений достовірний канал	Реалізується, так як використовується користувачем логін і пароль для входу в систему. Зв'язок з використанням даного каналу відбувається виключно користувачем, а не роботом.
НО-1. Виділення адміністратора	Реалізується, так як визначаються ролі адміністратора і звичайного користувача.
НЦ-2. КЗЗ з гарантованою цілісністю	Виконується, тому що КЗЗ має власного домену для підтримання захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.
НТ-2. Самотестування при старті	Реалізується, бо йде перевірка файлів при запуску системи.
НВ-1: Автентифікація вузла	Виконується, так як йде оновлення операційної системи з офіційних серверів постачальника ОС.

Таблиця 1.12 – Критерії, що не виконуються

Критерії	**Пояснення**
НИ-1. Зовнішня ідентифікація і автентифікація	Не виконується, так як КЗЗ з використанням захищеного механізму не одержує від зовнішнього джерела логін і пароль користувача.
НО-2. Розподіл обов'язків адміністраторів	Не реалізується, так як у нас один адміністратор.

1.5 Постанова задач.

Під час виконання першого розділу, було виконано обґрунтування створення необхідності комплексної системи захисту інформації, встановлено, яка інформація циркулює у ТОВ «Охоронна фірма СТІНА» згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» у ТОВ «Охоронна фірма СТІНА» циркулює інформація з обмеженим доступом (персональні данні персоналу та клієнтів), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником. Необхідно розробити ефективну політику безпеки за для мінімалізації ризиків інформаційної системи.

1.6 Висновки

Були розглянуті загальні відомості про підприємство, проведено обстеження об’єкту інформаційної діяльності, зроблена класифікація інформації, зроблений аналіз інформаційних потоків, що циркулюють на підприємстві, виконаний аналіз загроз та вразливостей системи, розроблена модель порушника, проведений аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності

Після обстеження об’єкту інформаційної діяльності ТОВ «Охоронна фірма СТІНА» та проведення аналізу ризиків стало відомо, що найбільший ризик для підприємства несуть загрози: крадіжка (копіювання) інформації та знищення інформації. Виходячи із таблиці 1.10 дані загрози мають найвищий рівень ризику, а саме 1.

2.2 Проектні рішення

Розробка політики безпеки

1 Мета політики безпеки

Встановити правила користування ІТС фірми, необхідні вимоги для роботи з конфіденційними файлами та інформацією. Всі користувачі, які використовують мережу для доступу до інформаційних ресурсів мають виконувати вимоги інструкції.

2 Область дії

Вимоги інструкції розповсюджуються на весь персонал ІТС ТОВ «Охоронна фірма СТІНА» , що користується нею.

3 Відповідальні особи

Відповідальним за дотримання інструкції системним адміністратором є директор фірми.

4 Інструкція

Перед підключенням до мережі на робочому ПК повинні бути встановленні критичні оновлення для операційної системи та програмного

забезпечення, також повинні бути встановленні актуальні бази даних антивірусних систем.

При оброці інформації користувач повинен контролювати щоб особи, які не мають прав на цю інформацію, не змогли несанкціоновано ознайомитися з нею з екрану монітора.

Користувач повинен ввести свої аутентифікаційні дані після підключені до мережі.

Паролі доступу до мережі відаються системним адміністратором після дозволу директора фірми.

Робочий ПК який використовується для доступу в ІТС повинен мати пароль для доступу до ОС.

Користувач повинен відключатися від мережі після завершення роботи з інформацією.

5 Затвердження політики безпеки

Після розробки політики безпеки системним адміністратором вона підписується директором фірми.

6 Дії з виконання інструкції

Системний адміністратор має контролювати усі підключення до мережі, та мати засоби моніторингу та виконання політики доступу.

7 Відповідальність за виконання інструкції

За виконання інструкції відповідальність несуть директор фірми та системний адміністратор.

Політика використання паролів

1 Мета політики

Мета цієї політики встановити стандарти створення надійних та сильних паролів, збереження та їх захист.

2 Область застосування

Політика використання паролів відноситься до всього персоналу, хто відповідальний за доступ до інформації усіх рівнів на будь якому обладнані яке має доступ до мережі.

3 Політика

3.1 Паролі облікових записів повинні змінюватись кожного кварталу.

3.2 Всі паролі від облікових записів повинні зберігатись в базі даних у зашифрованому вигляді, доступ до якої повинен бути обмежений.

3.3 Термін дії паролів повинен становити не більше 9 місяців.

3.4 Пароль користувача який має привілеї повинен бути унікальним від інших паролів.

4 Інструкція створення паролів

Користувачі фірми використовують паролі для різних цілей. Тому слід знати як вибрати надійний та стійкий пароль.

Слабким паролям притаманні такі ознаки:

- складаються менше ніж з восьми символів;
- містять особисту інформацію користувача таку як: улюблена страва, країна народження, кличку домашньої тварини;
- являє собою слово яке міститься у словнику.

Інструкція з організації антивірусного захисту

1 Загальні положення

Для забезпечення безпеки інформації допускаються до використання тільки ліцензійне антивірусні засоби придбанні у постачальників або напряму у розробника.

Антивірусні засоби які не увійшли до списку рекомендованих слід узгодити з системним адміністратором про їх застосування.

Встановлення антивірусних засобів на персональний комп'ютер здійснюється системним адміністратором. Налаштування антивірусних засобів здійснюється системним адміністратором.

2 Застосування антивірусного забезпечення

Обов'язковому антивірусному контролю підлягають усі персональні комп'ютери та інформація отримана або передана по телекомунікаційних каналах.

Антивірусний контроль персонального комп'ютера повинен проводитися щоденно при завантаження ПК.

Оновлення баз даних антивірусних засобів повинно проводитися регулярно у автоматичному режимі при завантаженні ПК.

У разі перевірки антивірусними засобами знаходження у системі вірусного програмного забезпечення співробітники фірми повинні:

- негайно припинити роботу та будь які дії на персональному комп'ютеру та сповістити системного адміністратора;

У разі перевірки знаходження віруса на персональному комп'ютеру системний адміністратор повинен:

- Забезпечити видалення вірусу з системи;
- У разі виявлення нового вірусу, що не піддається лікуванню антивірусними засобами які застосовувались, системний адміністратор повинен направити заражений файл вірусом до організації, з якою укладено договір на підтримку антивірусного забезпечення.

Користувачеві ІТС забороняється встановлювати прикладного та системного програмного забезпечення без схвалення системним адміністратором.

Перед встановленням програмне забезпечення повинно бути перевірено на відсутність вірусів.

Після встановлення програмного забезпечення ІТС повинна проводитися антивірусна перевірка.

Користувач зобов'язаний:

- При початкованому завантаженні ПК переконатися в наявності резидентного антивірусного монітора, у разі його відсутності повідомити про це системного адміністратора;
- Самостійно запускати позапланову антивірусну перевірку ПК при отримані повідомлення від системного адміністратора о наявності віруса в системі або на виникненні підозри про наявність віруса.

3 Відповідальність

За організацію антивірусного контролю ІТС покладається на директора фірми.

За проведення заходів з антивірусного контролю та дотримання вимог цієї інструкції відповідальність покладається на відповідального за забезпечення інформаційної безпеки і всіх співробітників які являються користувачами ІТС фірми.

Системний адміністратор несе відповідальність за контроль за станом антивірусного захисту фірми, а також за виконанням співробітниками даної інструкції.

За порушення вимог цього документа співробітник фірми притягується до відповідного до чинного законодавства України.

Інструкція щодо захисту підприємства від внутрішніх загроз для бухгалтера

1 Підписати угоду щодо нерозголошення інформації, яка становить комерційну таємницю, що є власністю ТОВ «Охоронна фірма СТІНА».

2 Везти облік у повному обсязі необоротних активів, запасів, коштів, розрахунків, доходів та витрат за прийнятою на підприємстві формою бухгалтерського обліку з додержанням єдиних методологічних засад бухгалтерського обліку та з урахуванням особливостей діяльності підприємства й технології оброблення даних.

3 Забезпечувати підготовку оброблених документів, реєстрів і звітності для зберігання їх протягом установленого терміну.

4 Готувати дані для включення їх до фінансової звітності, здійснює складання окремих її форм, а також форм іншої періодичної звітності, яка грунтується на даних бухгалтерського обліку.

Інструкція щодо захисту підприємства від внутрішніх загроз для директора фірми

1 Здійснювати заходи щодо соціального захисту колективу підприємства, забезпечення і збереження зайнятості працівників.

2 Вирішувати всі питання в межах наданих йому прав, доручати виконання окремих організаційно-господарських функцій іншим посадовим особам: заступникам керівника, керівникам виробничих підрозділів підприємства.

3 Вживати заходи щодо забезпечення підприємства кваліфікованими кадрами, найкращого використання безпечних і сприятливих умов праці.

4 Визначати, формулювати, планувати, здійснювати і координувати всі види діяльності підприємства.

5 Направляти діяльність персоналу на досягнення високих економічних та фінансових результатів.

Інструкція щодо захисту підприємства від внутрішніх загроз для заступника директора фірми

1 Організовувати роботу і ефективну взаємодію всіх структурних підрозділів, цехів та виробничих одиниць, підвищує рентабельність фірми.

2 Контролювати роботу всіх структурних підрозділів фірми.

3 Затверджувати штатний розклад фірми, встановлює посадові оклади та надбавки щокварталу або в міру необхідності.

4 Проводити роботи з удосконалення планування економічних і фінансових показників діяльності підприємства, по створенню й поліпшенню нормативів трудових витрат, витрачання товарно-матеріальних цінностей і використання виробничих потужностей.

5 Здійснювати контроль за порядком обліку надходження і витрачання коштів, використанням матеріальних цінностей.

6 Забезпечувати контроль за ходом дотримання фінансової дисципліни.

7 Контролювати своєчасність подання звітності про результати економічної звітності про результат економічної діяльності в установленому порядку та терміни на розгляд директору.

Інструкції щодо захисту підприємства від внутрішніх загроз для системного адміністратора

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «Охоронна фірма СТІНА».

2 Забезпечувати конфіденційність, цілісність, доступність комп’ютерних баз даних.

3 Здійснювати систематичний аналіз керованих апаратних засобів і програмного забезпечення.

4 Усувати аварійні ситуації, пов’язані з пошкодженням ПЗ та баз даних.

5 Впровадити на сервері міжмережевий екран для фільтрації можливого шкідливого трафіку.

6 Забезпечити застосування системи резервного копіювання.

7 Затвердити усі програми, що використовуються для доступу до мережі Internet і налаштувати на них необхідні рівні безпеки.

8 Забезпечувати безперервну роботу серверу.

9 Створювати та змінювати паролі на всі робочі станції та облікові записи домену та на персонал, що з ними працює.

10. Створювати пароль відповідно до вимог «Політики використання паролів».

Інструкції щодо захисту підприємства від внутрішніх загроз для менеджера з продажу

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «Охоронна фірма СТІНА».

2 Виконувати роботу з укладання договорів на постачання послуг і узгодження умов.

3 Вживати заходів із забезпечення своєчасного надходження коштів за реалізовану продукцію.

4 Організовувати зв'язки з діловими партнерами, забезпечувати своєчасне виконання обов'язків перед контрагентами, добирати необхідну інформацію для розширення зовнішніх зв'язків

5 Контролювати внесення змін у довідкову та рекламну інформацію.

Інструкції щодо захисту підприємства від внутрішніх загроз для секретаря

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «Охоронна фірма СТІНА».

2 Приймати кореспонденцію, яка надходить на розгляд директору підприємства, передає її згідно з прийнятим рішенням до структурних підрозділів або конкретним виконавцям для використання в процесі роботи або підготовки відповідей.

3 Готувати документи і матеріали, необхідні для роботи директорові підприємства.

4 Стежити за своєчасним розглядом і поданням структурними підрозділами та конкретними виконавцями документів, що надходять для виконання, перевіряти правильність оформлення підготовлених проектів документів, що передаються керівнику на підпис, забезпечути їх якісне редагування.

5 Здійснювати контроль за виконанням працівниками підприємства виданих наказів та розпоряджень, а також за додержанням термінів виконання вказівок і доручень директора підприємства, що взяті на контроль.

6 Організовувати проведення телефонних переговорів директора підприємства, записує за його відсутності одержану інформацію і доводить до його відома її зміст, передає і приймає інформацію за допомогою приймально-переговорних пристроїв (телефакс, телекс, і т. ін.), а також телефонограми, своєчасно доводить до відома директора підприємства інформацію, одержану каналами зв’язку.

7 Везти діловодство, виконувати різні операції із застосуванням комп’ютерної техніки, призначеної для збирання, оброблення і подання інформації для підготовки і прийняття рішень.

Інструкції щодо захисту підприємства від внутрішніх загроз для начальника охорони

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «Охоронна фірма СТІНА»

2 Координувати роботу охорони, керувати діями охоронців при виникненні нештатних ситуацій.

3 Забезпечувати дотримання надійного контрольно-пропускного режиму.

4 Здійснювати затримку осіб, що намагаються незаконно вивезти (винести) матеріальні цінності з охоронюваного об'єкта або підозрюваних у здійсненні правопорушень.

5 Щоденно контролювати здавання та приймання під охорону обладнаних сигналізацією відособлених приміщень.

6 Припиняти спроби несанкціонованого проникнення на охоронюваний об'єкт.

Інструкції щодо захисту підприємства від внутрішніх загроз для співробітника служби безпеки

1 Підписати угоду щодо нерозголошення конфіденційної інформації, що є власністю ТОВ «Охоронна фірма СТІНА»

2 У разі виявлення порушень норм терміново повідомляти про це представника власника об’єкта або уповноваженого ним органу.

3 Приймати та здійснює вантажі з відповідними документами.

4 Під час охорони стаціонарних об’єктів із встановленим пропускним режимом пропускати працівників, відвідувачів, автомобільний та інші види транспорту і випускає їх із території об’єкта в установленому порядку і за зразками документів, затверджених власником об’єкта або уповноваженим ним органом.

5 За особливими умовами договору ведзти реєстрацію показань приладів екологічної та локальної пожежної безпеки, наглядати за устаткуванням, яке встановлено на об’єкті, що охороняється, додержуючись чинних норм з охорони праці.

Інструкція з використання електронних ресурсів комп’ютерної мережі

1 Загальні положення

1.1 Метою цієї інструкції є регулювання роботи системного адміністратора і користувачів, розподілу мережевих ресурсів колективного користування та підтримки необхідного рівня захисту інформації, її збереження, і дотримання прав доступу до інформації. Більш ефективного використання мережевих ресурсів і зменшення ризику навмисного чи ненавмисного неправильного їх використання.

1.2 До роботи в системі допускаються особи, призначені начальником відділу, які пройшли інструктаж та реєстрацію.

1.3 Робота в системі кожному працівникові дозволена тільки на певних комп’ютерах і тільки з дозволеними програмами і мережевими ресурсами. Якщо потрібно працювати на інших комп’ютерах і з іншими програмами, необхідно отримати дозвіл системного адміністратора.

1.4 Кожен користувач створює пароль для входу в комп’ютерну мережу. При цьому пароль повинен містити мінімум 8 символів, містити букви і цифри.

1.5 Кожен користувач повинен користуватися лише своїм іменем користувача та паролем для входу в локальну мережу та мережу Інтернет, передача їх будь-кому заборонено.

1.6 Для роботи на комп’ютері окрім користувача необхідний дозвіл системного адміністратора. Ніхто не може давати дозвіл на навіть

тимчасову роботу на комп’ютері, без дозволу системного адміністратора або начальника відділу.

1.7 У разі порушення правил користування мережею, користувач повідомляє системного адміністратора, який проводить розслідування причин і виявлення винуватців порушень і вживає заходи щодо припинення подібних порушень. Якщо винуватцем порушення є користувач даного комп’ютера, адміністратор має право відсторонити винуватця від користування комп’ютером або вжити інші заходи.

1.8 Системний адміністратор – особа, що обслуговує сервер і стежить за правильним функціонуванням мережі. Системний адміністратор дає дозвіл на підключення комп’ютера до мережі, видає IP-адреса комп’ютера, створює обліковий запис електронної пошти для користувача. Самовільне підключення є серйозним порушенням правил користування мережею.

2 Обов’язки користувачів мережі

2.1 Дотримуватися правил роботи в мережі, обумовлені цією інструкцією.

2.2 При доступі до зовнішніх ресурсів мережі, дотримуватися правил, встановлених системними адміністраторами для використовуваних ресурсів.

2.3 Негайно повідомляти системного адміністратора про виявлені проблеми у використанні наданих ресурсів, а також про факти порушення цієї інструкції ким-небудь. Адміністратор, при необхідності, за допомогою інших фахівців, повинен провести розслідування зазначених фактів і вжити відповідних заходів.

2.4 Не розголошувати відому їм конфіденційну інформацію (імена користувачів, паролі), необхідну для безпечної роботи в мережі.

2.5 Негайно відключати від мережі комп’ютер, який підозрюється в зараженні вірусом. Комп’ютер не повинен підключатися до мережі до тих пір, поки системний адміністратор не переконаються у видаленні вірусу.

2.6 Виконувати приписи, спрямовані на забезпечення безпеки мережі.

3 Заборонено

3.1 Дозволяти стороннім особам користуватися довіреним їм комп’ютером.

3.2 Використовувати мережеві програми, не призначені для виконання прямих службових обов’язків без узгодження з системним адміністратором.

3.3 Самостійно встановлювати або видаляти встановлені системним адміністратором мережеві програми на комп’ютерах, змінювати налаштування операційної системи та програм, що впливають на роботу мережевого обладнання та мережевих ресурсів.

3.4 Пошкоджувати, знищувати або фальсифікувати інформацію, що не належить користувачу.

3.5 Самовільно підключати комп’ютер до мережі, а також змінювати IP-адреса комп’ютера, виданий системним адміністратором.

Отже, для мінімізації загроз «Крадіжка (копіювання) інформації» та «Знищення інформації», які були виявлені на етапі «Аналіз ризиків», потрібно виконати заходи що зазначені в розроблених інструкціях політики інформаційної бзпеки:

1 Використання надійних паролів та їх регулярна зміна;

2 Встановити надійного антивірусного програмного забезпечення;

3 Встановити систему безпеки з контролем доступу;

4 Встановити міжмережевого екрану, для контролю потоку інформації з/у захищаємої мережі;

Впровадження системи контролю і безпеки робочих станцій, для усунення загрози, зв’язаної з несанкціонованою користувачевою активністю (ESET Endpoint Security);

Аналіз ризиків після впровадження політики безпеки

Розглянемо таблицю 2.13, в ній показано, як змінилися показники ризиків після застосування інструкцій політики безпеки.

Таблиця 2.13 – Аналіз ризиків після впровадження політики безпеки

Загрози	**Наслідки (b)**	**Імовірність поширення загроз (c)**	**Міра ризику (d)**	**Ранжування загрози (e)**
Крадіжка (копіювання) інформації	2	2	4	2
Знищення інформації	3	1	3	2
Змінення інформації	2	1	2	3
Порушення доступності (блокування) інформації	2	1	2	3
Заперечення достовірності інформації	1	1	1	3
Нав’язування помилкової інформації	1	1	1	3

Для стовпців «b» і «c»:

1 – низький; 2 – середній; 3 – високий.

Для стовпця «e»:

1: 5 – 6 – високий;

2: 3 – 4 – середній;

3: 1 – 2 – низький.

Загрози «Крадіжка (копіювання) інформації» та «Знищення інформації», що представляли найбільший ризик для підприємства, котрі були виявлені у пункті «Аналіз ризиків», тепер мають інші показники, менші, ніж до того, як були застосовані інструкції.

Тож тепер «Крадіжка (копіювання) інформації» має оцінку «Ранжування загрози» 2, що означає середній рівень, замість 1 – високого. Та загроза «Знищення інформації» має також середній рівень, замість високого.

2.3 Висновки

Під час виконання другого розділу було створено політику безпеки для ТОВ «Охоронна фірма СТІНА», після впровадження якої дозволило зменшити оцінку ризику для таких загроз як крадіжка (копіювання) інформації та знищення інформації з високого рівня ризику (1) до середнього рівня ризику (2)

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Згідно розд. 2.2 для мінімізації загроз «Крадіжка (копіювання) інформації» та «Знищення інформації», які були виявлені на етапі «Аналіз ризиків», потрібно виконати заходи що зазначені в розроблених інструкціях політики інформаційної безпеки:

1 Використання надійних паролів та їх регулярна зміна;

2 Встановити надійного антивірусного програмного забезпечення;

3 Встановити систему безпеки з контролем доступу;

4 Встановити міжмережевого екрану, для контролю потоку інформації з/у захищаємої мережі;

5 Впровадження системи контролю і безпеки робочих станцій, для усунення загрози, зв’язаної з несанкціонованою користувачевою активністю (ESET Endpoint Security);

3.1 Розрахунок капітальних витрат на програмне та апаратне забезпечення

В табл. 3.1 вказана вартість активів, що планується придбати для встановлення у відділі продажу згідно розробленої політики інформаційної безпеки.

Таблиця 3.1 – Витрати на придбання матеріальних та нематеріальних активів

№	Назва продукту	Вартість
1	Міжмережевий екран	11 300 грн.
2	Антивірусна програма з вбудованим міжмережевим екраном ESET NOD32 Smart Security	2960,00 грн.
3	Програма резервного копіювання та відновлення Acronis Backup & Recovery 11 Advanced Server	9630,00 грн.
4	ESET Endpoint Security. Первоначальное приобретение на 5 лет на 6 ПК Джерело http://softlist.com.ua/personal/basket/	18100 грн.
Всього		41990 грн.

Капітальні витрати - грошові видатки, пов'язані з вкладеннями в основний капітал чи в приріст виробничих запасів. Витрати на розробку політики інформаційної безпеки наведені в табл. 3.2.

Таблиця 3.2 – Трудомісткість та витрати на розробку політики інформаційної безпеки

Склад витрат	Трудомісткість, год-осіб	Вартість грн./год.-осіб з податками	Сума, грн
Обстеження ОІД	8	70,00	560
Аналіз загроз та уразливостей	5		350
Розробка моделі порушника	4		280
Аналіз ризиків	3		210
Розробка профілю захищеності	10		700
Розробка політики безпеки	12		840
Розробка політики використання паролів	12		840
Розробка інструкції з організації антивірусного захисту	18		1260
Розробка інструкції щодо захисту підприємства від внутрішніх загроз для бухгалтера	12		840
Розробка інструкції щодо захисту підприємства від внутрішніх загроз для системного адміністратора	25		1750
Розробка інструкції з використання електронних ресурсів комп’ютерної мережі	15		1050
Всього			8680,00

Сумарні капітальні витрати на розробку та реалізації політики інформаційної безпеки складає:

41990+8680=50 670 грн

3.2 Розрахунок експлуатаційних витрат

Додаткових поточних витрат на електроенергію та заробітну платню обслуговуючого персоналу не потребує. При зміні паролів кожний місяць для 10 осіб додаткові витрати не передбачені, що обґрунтовується тим, що паролі

будуть змінені протягом 1 робочого дня. Тому поточні витрати складаються тільки з амортизаційних витрат з урахуванням строку службі 12 років (9 група основних засобів згідно п.138,1 Податкового кодексу України) та додаткових витрат на надання та зміну паролів. Виходячи з цього поточні річні витрати:

Саморт = К/12 = 50670/12 =4223 грн

3.3 Оцінка можливого збитку від витоку або пошкодження інформації

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина *відвернених втрат*, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента мережі, годин;

$З_о$ – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента мережі, осіб.;

O – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента мережі;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів мережі;

N – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

$$U = П_п + П_в + V, \tag{3.1}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п, \tag{3.2}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

Витрати на відновлення працездатності вузла або сегмента мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \tag{3.3}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} \qquad (3.4)$$

Витрати на відновлення вузла або сегмента мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \ . \qquad (3.5)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента мережі визначаються виходячи із середнього динного обсягу продажів і сумарного часу простою атакованого вузла або сегмента мережі:

$$V = \frac{О}{F_г} \cdot (t_п + t_в + t_{ви}) \quad , \qquad (3.6)$$

де $F_г$ – річний фонд часу роботи торгівельного підприємства (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент мережі торгівельного підприємства складе

$$B = \sum\sum U \cdot I \, . \qquad (3.7)$$

Штат співробітників відділу складає 5 осіб + системний адміністратор. Середня годинна заробітна плата на підприємстві з урахуванням єдиного соціального внеску 64,92 грн/год.

Отже вихідні дані:

- $t_п = 26$ годин;

- $t_в = 9$ годин;
- $t_{ви} = 13$ годин;
- Q=2665332 грн. згідно інформації, наведеної в аудиторському звіті за 2018 рік http://www.nzf.com.ua/files/audit2017.pdf;
- $П_{зч} = 0$ грн.;
- I=1.

Згідно формулою (3.2) – (3.6):

Пп=64,92*9*26=15191 грн.

Пви=64,92*9*9=5259 грн.

Ппв=64,92*1*13=844грн.

Пв=5259+844+0=6103 грн.

V=2665332/2080*(26+9+13)=61507 грн

Згідно з формулою (3.1) та (3.7) отримаємо:

U=15191+6103+61507 = 82801грн.

При 1 атаці B=82801 грн

3.4 Загальний ефект від впровадження системи управління інформаційної безпеки

Загальний ефект від впровадження системи управління інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

*E=B*R-C=82801*0,5-4223=37177.5*

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = E/K = 37177.5/50670 = 0.73$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$To=K/E=1/ROSI=50670/37177.5=1/0.73$$

$$1.36=1.36 \text{ року}$$

При вирогідності 50% система інформаційної безпеки окупиться за 1,5 року.

3.6 Висновки

У цьому розділі обґрунтована економічна доцільність використання приведеної у дипломній роботі розробленої політики інформаційної безпеки для ТОВ «Охоронна фірма СТІНА». При одноразових капіталовкладеннях у розмірі 50 670 грн, коефіцієнт окупності є 0.73 (ROSI), що означає окупність розробки політики безпеки за 1.5 року. Максимальні витрати при реалізації загрози становлять 81801 грн.

ВИСНОВКИ

В ході виконання дипломного проекту був проведений аналіз нормативно-правової бази України у сфері захисту інформації, розглянуті державні, а також міжнародні стандарти, за допомогою яких регулюються інформаційні відносини на підприємстві, забезпечуються норми зберігання, обробки, поширення інформації.

Було виконано:

– обстеження об’єкту інформаційної діяльності;

– аналіз інформаційних потоків;

– аналіз загроз та вразливостей системи;

– побудована модель порушника;

– аналіз ризиків для виявлення слабких місць у системі забезпечення інформаційної безпеки;

– обґрунтування вибору стандартного функціонально профіля захищеності;

– аналіз виконання вимог стандартного функціонального профіля захищеності;

– розроблені інструкції політики безпеки, для мінімізації реалізації ризиків втрати, викривлення, розголошення інформації, яка несе у собі життєвоважливі інтереси для підприємства.

Також було виконано обґрунтування створення необхідності комплексної системи захисту інформації, встановлено, яка інформація циркулює у ТОВ «Охоронна фірма СТІНА», згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» у ТОВ «Охоронна фірма СТІНА» циркулює інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником.

СПИСОК ЛІТЕРАТУРИ

1 Литюга Ю. В «Організація ризик-менеджменту на підприємстві». - IV Міжнародна науково-практична конференція «ЕКОНОМІКА ПІДПРИЄМСТВА: ТЕОРІЯ І ПРАКТИКА», Київський національний економічний університет імені Вадима Гетьмана, 2012 / Спосіб доступу: URL: http://kneu.edu.ua/ua/departments/ Faculty_of_Economics_and_Administration/confere_nce/ec_pidpr_th_pr_4/sect5/. - Загол. з екрана;

2 Електронний курс eNano, Сидоренко О. П. «Управління ризиками для підприємців»/ Спосіб доступу: URL: http://www.intuit.ru/studies/courses/ 4456/715/info. – Загол. з екрана;

3 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

4 Про захист інформації інформаційно-телекомунікаційних системах: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

5 Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту: [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua.

6 Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие / Хорев А.А., 1998. – 320 с.

7 Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навч. посібник. – К.: Юстініан, 2006. – 176 с.

8 Хорев А.А. Методы и средства поиска электронных устройств перехвата информации, 1998. – 224 с.

9 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 1999 – 16 с.

10 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТС31 СБ України, 1999. - 26 с.

11 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» НД ТЗІ 3.7-003-2005 [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/

12 Міжнародний стандарт ISO / IEC 27001:2013 «Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки - Вимоги»

13 Про інформацію: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

14 Про телекомунікації: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

15 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

16 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт, можна встановити вимоги щодо порядку проведення робіт з технічного захисту інформації (ТЗІ).

17 Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.

18 Літнарович Р. М. Сучасні технології інформаційної безпеки – Навчальний посібник – Рівне 2011.

19 Лазарев Г. Захист інформації в інформаційно-телекомунікаційних системах // Національна безпека і оборона. — К.: 2001. — № 1. — С. 80-83.

Пугин В.В., Губарева О.Ю. – «Обзор методик анализа рисков информационной безопасности информационной системы предприятия».

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	2	
5	А4	1 Розділ	37	
6	А4	2 Розділ	15	
7	А4	3 Розділ	7	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на дипломну роботу бакалавра на тему:
Розробка політики безпеки інформації
студента групи УБіт-15-1
Олешко Єгора Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках, та містить __ рисунків, __ таблиць, __ джерел та __ додатків.

Об'єкт розробки: інформаційно-телекомунікаційна система ТОВ «Охоронна фірма СТІНА».

Предмет дослідження: політика безпеки інформації об'єкта інформаційної діяльності.

Мета дипломного проекту: розробка політики безпеки для підприємства ТОВ «Охоронна фірма СТІНА».

В роботі виконане обстеження ОІД, інформаційного середовища та обчислювальної системи. Наведена класифікація циркулюючої інформації.

На підставі зібраних даних була розроблена модель порушника і модель загроз, та зроблено аналіз ризиків.

Після чого був обраний профіль захищеності і розроблена політика безпеки. Після впровадження політики безпеки був ще раз проаналізований рівень ризиків, і було визначено, що він зменшився.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор знає проблему, уміє формулювати практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку **«70» балів.**

Керівник дипломної роботи,
д.т.н., проф. В.І. Корнієнко